PRIVACY IMPACT ASSESSMENT (PIA)

For the

Defense Travel System (DTS)
Defense Manpower Data Center

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐ **New DoD Information System** ☐ **New Electronic Collection**

☒ **Existing DoD Information System** ☐ **Existing Electronic Collection**

☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☒ **Yes, DITPR** Enter DITPR System Identification Number 125

☐ **Yes, SIPRNET** Enter SIPRNET Identification Number

☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☒ **Yes** ☐ **No**

If "Yes," enter UPI 007-97-01-31-01-6312-00

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒ **Yes** ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DMDC 28 DoD

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. Pending

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☒ **Yes**

Enter OMB Control Number 60-day PRA Notice XXXXXX

Enter Expiration Date

☐ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

5 U.S.C. 57, Travel, Transportation, and Subsistence; DoD Directive 5100.87, Department of Defense Human Resources Activity; DoD Instruction 5154.31, Volume 3, Commercial Travel Management: Defense Travel System (DTS); DoD Financial Management Regulation 7000.14-R, Vol. 9, Defense Travel System Regulation, current edition; DoD Directive 4500.09E, Transportation and Traffic Management; DTR 4500.9-R, Defense Transportation Regulation, Parts I, Passenger Movement, II, Cargo Movement, III, Mobility, IV, Personal Property, V, Customs; 41 C.F.R. 300-304, The Federal Travel Regulation (FTR); Joint Federal Travel Regulations, Uniformed Service Members and DoD Civilian Employees; and E.O. 9397 (SSN), as amended.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

DTS provides a DoD-wide travel management system to include the processing of official travel requests for DoD personnel and other individuals who travel pursuant to DoD travel orders; to provide for the reimbursement of travel expenses incurred by individuals while traveling on official business; and to create a tracking system whereby DoD can monitor the authorization, obligation, and payment for such travel.

DTS includes a business intelligence tool and archive that provide a repository for reporting and archiving travel records and can be used to satisfy reporting and records management requirements. It is used to analyze travel and budgetary trends, respond to requests for data related to travel, and detect fraud and abuse. The DTS Pilot Program (DTSPP) evaluates more modern technology, common practices of the travel industry, and the feasibility of a commercial travel product to make DoD travel operations more efficient. It has a limited scope that minimizes the collection of sensitive PII.

DTS collects the following types of personal information: full name, Social Security Number (SSN), DoD Identification Number (DoDID), gender, date of birth, Passport information, mailing address, home address, emergency contact information, and personal email address. It collects employment information including Service/Agency, duty station information, title/rank, civilian/military status information, and work email address. It collects financial information including the government travel card number and expiration date, personal credit card number and expiration date, and personal checking and/or savings account numbers and bank routing information. And it collects travel information including frequent flyer information, travel itineraries (includes dates of travel) and reservations, trip record number, trip cost estimates, travel vouchers, travel-related receipts, travel document status information, travel budget information, commitment of travel funds, records of actual payment of travel funds, and supporting documentation.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The risks are exposure of PII data to unauthorized personnel without a need to know. The risk is mitigated through a combination of physical, technical, and administrative controls. Records are stored in office buildings protected by security guards, closed circuit TV, controlled screening, use of visitor registers, electronic access, key cards, ID badges, and/or locks. Access to the systems data is controlled using intrusion detection systems, firewalls, a virtual private network, and DoD PKI certificates. Procedures are in place to deter and detect browsing and unauthorized access. To access the records, personnel are assigned role-based access and must complete two-factor authentication using a CAC credential and password/PIN. Access to records is limited to individuals who are properly screened and cleared on a need-to-know basis in the performance of their official duties. Physical and electronic access are limited to persons responsible for servicing and authorized to use the record system. The backups of data are encrypted and secured. The program office conducts security audits and monitor security practices.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☒ **Other DoD Components.**

Specify. All DOD components use DTS and have access to their own data stored within the system. Defense Travel Management Office (DTMO) also uses travel data metrics for inquiries and program management.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. The DTS operations and maintenance contractors and DTS PMO support contractors comply with the requirements of OMB Memorandum M-06-16, Protection of Sensitive Agency Information, DoD Memorandum of June 23, 2006, DoD Guidance on Protecting PII, and DHRA Policy and Procedures When Personal Information is Lost, Stolen or Compromised. DTS contractors access information on an as-needed basis to troubleshoot system issues and respond to program inquiries.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

If individuals object to the collection of their PII, then they should not enter the DTS system or accept the disclosure upon DTS login. They may request a manual itinerary generation to reduce the amount of PII that is collected, however, ultimately, if they choose to travel on DoD orders, they must allow the collection of PII. The privacy notice presented to the user prior to login states “DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and the claim for reimbursement.”

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

Individuals have opportunity to consent before entering the site by clicking “accept” on the Privacy and Ethics Policy banner page. Once stored within the system, use of the data is controlled by the DTS application, not by the user.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.

The following Privacy Act Statement is presented to the individual upon access the DTS login page. The statement is presented electronically on the web-based application.

PRIVACY ACT
AUTHORITY: 5 U.S.C. 57, Travel, Transportation, and Subsistence; DoD Directive 5100.87, Department of Defense Human Resources Activity; DoD Instruction 5154.31, Volume 3, Commercial Travel Management: Defense Travel System (DTS); DoD Financial Management Regulation 7000.14-R, Vol. 9, Defense Travel System Regulation, current edition; DoD Directive 4500.09E, Transportation and Traffic Management; DTR 4500.9-R, Defense Transportation Regulation, Parts I, Passenger Movement, II, Cargo Movement, III, Mobility, IV, Personal Property, V, Customs; 41 C.F. R. 300-304, The Federal Travel Regulation (FTR); Joint Federal Travel Regulations, Uniformed Service Members and DoD Civilian Employees; and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): The purpose of DTS is to provide a DoD-wide travel management process which will cover all official travel, from pre-travel arrangements to post-travel payments. The system facilitates the processing of official travel requests for DoD personnel and other individuals who travel pursuant to DoD travel orders. DTS provides information to financial systems to provide the reimbursement of travel expenses incurred by individuals while traveling on official business. DTS includes a tracking and reporting system whereby DoD can monitor the authorization, obligation, and payment for such travel. The DTS pilot program evaluates more modern technology, common practices of the travel industry, and the feasibility of a commercial travel product to make DoD travel operations more efficient.

ROUTINE USE: To Federal and private entities providing travel services for purposes of arranging transportation and lodging for those individuals authorized to travel at government expense on official business. To the Internal Revenue Service to provide information concerning the pay of travel allowances which are subject to federal income tax. To banking establishments for the purpose of confirming billing or expense data. See the applicable system of records notice for a complete listing of routine uses: DMDC 28 DoD, Defense Travel System (DTS) located at http://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/OSDJS-Article-List/

DISCLOSURE: Voluntary, however, failure to provide all of the requested information may preclude the processing of both the travel request and the claim for reimbursement.

DEPARTMENT OF DEFENSE: Department of the Army Narrative Statement on a New System of Records Under the Privacy Act of 1974.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.